The Sniffer™

The Case of "Slower is Faster"

Case #1801

The DECnet Sniffer Protocol Analyzer in action - how slowing down a system can make it work faster!

This is a case history in which The Sniffer by Network General was used to develop an understanding of a serious response time delay occurring during certain file transfers in an Ethernet system running DECnet protocols. Knowing the reason for the problem, it was possible to identify several ways to cure it, gaining a 25 to 1 improvement in response time. Some cures were costly, others far more economical.

Before we dig into the case itself, let us take a few moments to describe The Sniffer. If you already understand how The Sniffer functions, we suggest you skip over this explanation.

A Thumb-nail Sketch of The Sniffer

The Sniffer is a self-contained, portable, performance analysis and diagnostic instrument capable of analyzing the protocol content of packets transmitted on the LAN it is plugged into. It CAPTUREs images of all or of selected frames (packets) into a working buffer, ready for immediate analysis. CAPTURE frame selection is based on lower level protocol content, node addresses, pattern matching, and/or frame error conditions.

Newly-captured traces (images) are immediately available for display and analysis. Filters based on node addresses, protocol content at all levels, and pattern matching, may be invoked to select all or a portion of the captured frames for display.

Protocol interpretation at all levels in the ISO model occurs during the DISPLAY analysis process, providing the user with tabularly-organized information respecting the protocol content of the selected frames expressed in normal English language, in addition to address and timing data.

Analyzed and displayed data may be output to hard copy printers. Some printouts are included below for this case history.

A wide range of Display Formats is provided to facilitate the interpretation of patterns of response found on the network. These menu-selectable formats range from high level SUMMARY views depicting up to 17 frames at a glance, to DETAIL views of individual frames with interpretation carried to the individual bit level, all characterized by an English language presentation. Conventional HEXadecimal display with ASCII or EBCDIC interpretation is another menu choice. These display modes may be invoked individually or in any combination.

The DISPLAY/SUMMARY mode offers a variety of display formats to facilitate problem identification, including a Two-Station format useful in analyzing Command/Response situations; a Two-Viewport format facilitating the comparison of widely separated areas of a data stream; and several timing displays, including Delta Time (time between successive frames), Relative Time (time from a marked frame), Absolute Time (time-of-day stamp), and Network Utilization (shows percent of the LAN bandwidth being used in the vicinity of the captured frame - a rolling average with user-selectable averaging period); plus Bytes and Cumulative Bytes.

Now, let us turn to *The Case of "Slower is Faster"*

Figure 1. We have included this figure to show the richness of information available to the user of a Sniffer. It is a hard-copy printout of one of the many forms of analysis provided by The Sniffer, in this case focussing on just one packet captured from a network. In The Sniffer itself, this information appeared in a two-window format, the upper window presenting the SUMMARY view; the lower, the DETAIL view. The DETAIL view, which is much longer than the space available in The Sniffer's video screen, can be examined in The Sniffer itself by scrolling up and down through the field of information. In the printout, we see the whole picture in one view.

The SUMMARY view of this particular packet shows four nested protocols - Data link control (DLC), DECnet Routing Protocol (DRP), Network Services Protocol (NSP), and Data Access Protocol (DAP). The DETAIL view presents a complete interpretation of each of these protocols, in a language (English) and a form readily understandable by most network system managers.

Figure 2. Now, let's turn our attention to a SUMMARY view that is uniquely The Sniffer's - a view that is perhaps best described as 'an aerial photograph' of LAN activity. This SUMMARY view contains just one line for each packet, and, among other parameters, identifies (in English) the highest level protocol in each frame - here, the DECnet DAP protocol because we have filtered out all non-DAP frames. Furthermore, this DISPLAY setup invokes The Sniffer's 'Two Station' capability, which is very useful when the sole or principal activity being examined is between just two addresses on the LAN. In this case, all the frames from station 7.45 (note the legend 'From 7,52' at the top of the figure) are displayed in the left-hand group, while those from station 7.52 are displayed in the right-hand group.

This SUMMARY view, at the DAP (Data Access Protocol) level, is showing the sequence of packets generated when one station, 7.45, copies a file from another, 7.52. In frame 383, a message is sent requesting that a file be opened. The opening is confirmed approximately 0.27 seconds later by packet 385. The actual data transfer begins in frame 394. Look at the 5 and 10 second long interruptions that took place around frames 412, 439, 456, and 472. In all, these delays add up to about 25 seconds during a file transfer that should take no more than a second.

Figure 3. This is still a 'Two Station' SUMMARY view, but this time at the lower NSP (Network Services Protocol) level. This is the actual data transport level for DECnet and shows in greater frame-by-frame detail a portion of the same file transfer we were looking at in Figure 2. We see that the sequences numbers of the packets (e.g. SEG=nn on the right hand side) are increasing, and corresponding acknowledgments (e.g. ACK=nn on the left hand side) are arriving quite rapidly. However by frame 402 although segments 7 through 9 have been transmitted by station 7.52, in over 5 seconds there has been no acknowledgement from station 7.45. At this point, segment 7 is retransmitted by station 7.52, and the attempt to transfer continues.

Conclusion: the delays appear in station 7.45, which does not always respond to data sent to it. Part of the reason may be that station 7.52 is well tuned: frames 400, 401 and 402 were sent with virtually no gaps. Station 7.45 can't always handle such closely spaced packets, probably due to hardware limitations.

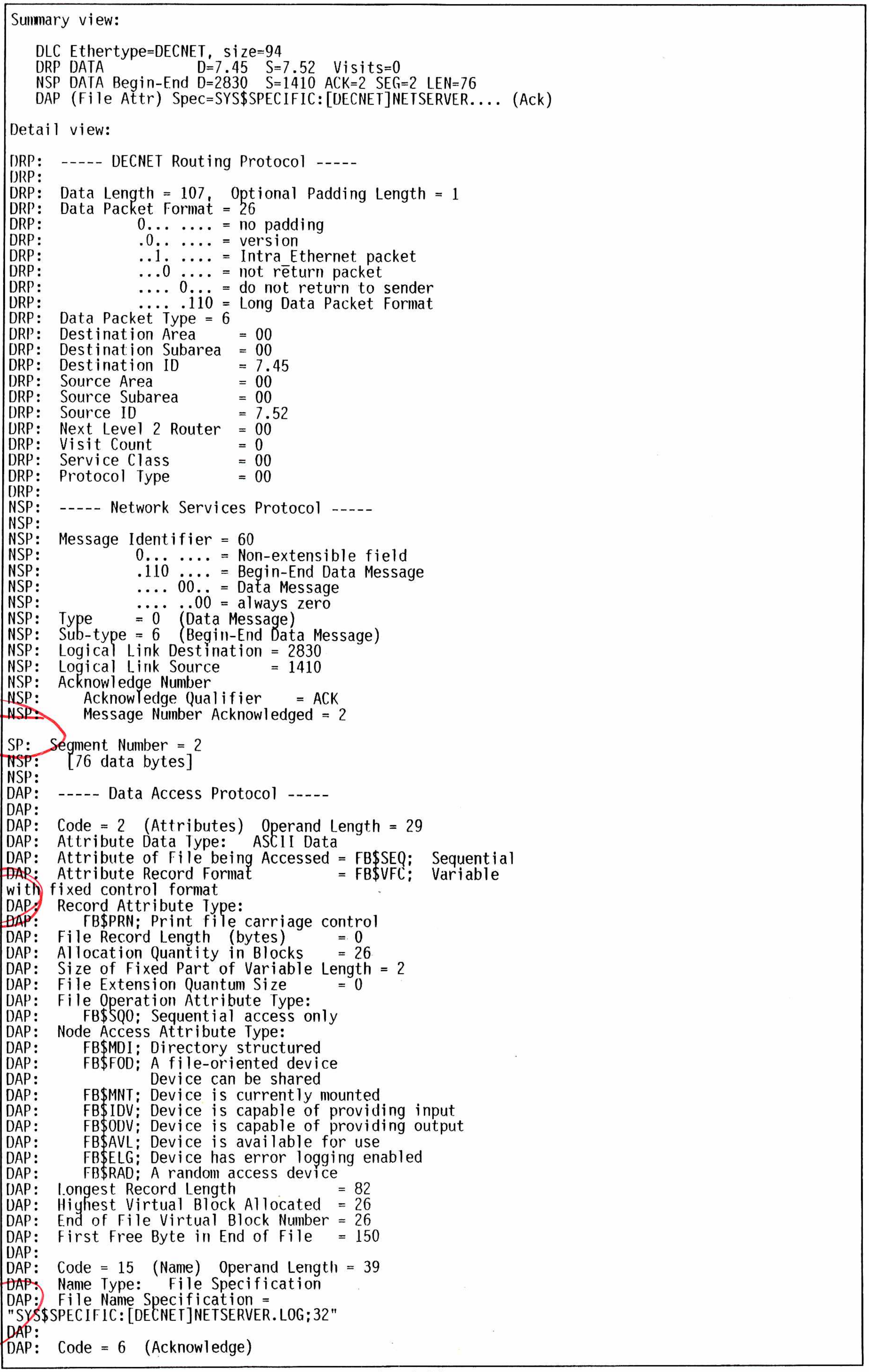
Faced with this situation, the system manager could either pick the brute force solution: install higher performance (and more expensive) equipment in station 7.45; or he/she could: A) modify the software or the hardware of station 7.52 to add slightly to the delay between the packets it sends; B) send somewhat shorter packets when transmitting to 7.45; or C) reduce the 5 second retry timeout.

Clearly, attempting to solve the problem by speeding up 7.52 will make things even worse. But slowing it down will solve the problem and will reduce twenty-five second file transfers to one second!

The paradox is resolved: ***Slower can be Faster!***

The Sniffer delivers a time advantage to its user. Its unique SUMMARY and DETAIL displays provide insights not available in other instruments, leveraging the professional investigator's time and knowledge. Users have reported solving problems in days that were previously taking weeks to bring under control; others, LAN end users as well as LAN equipment and software developers, have told us that their Sniffers paid for themselves on their first projects.

Figure 1.



```
Summary view:

   DLC Ethertype=DECNET, size=94
   DRP DATA           D=7.45  S=7.52  Visits=0
   NSP DATA Begin-End D=2830  S=1410 ACK=2 SEG=2 LEN=76
   DAP (File Attr) Spec=SYS$SPECIFIC:[DECNET]NETSERVER.... (Ack)

Detail view:

DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data Length = 107,  Optional Padding Length = 1
DRP:  Data Packet Format = 26
DRP:           0... .... = no padding
DRP:           .0.. .... = version
DRP:           ..1. .... = Intra_Ethernet packet
DRP:           ...0 .... = not return packet
DRP:           .... 0... = do not return to sender
DRP:           .... .110 = Long Data Packet Format
DRP:  Data Packet Type = 6
DRP:  Destination Area      = 00
DRP:  Destination Subarea   = 00
DRP:  Destination ID        = 7.45
DRP:  Source Area           = 00
DRP:  Source Subarea        = 00
DRP:  Source ID             = 7.52
DRP:  Next Level 2 Router   = 00
DRP:  Visit Count           = 0
DRP:  Service Class         = 00
DRP:  Protocol Type         = 00
DRP:
NSP:  ----- Network Services Protocol -----
NSP:
NSP:  Message Identifier = 60
NSP:           0... .... = Non-extensible field
NSP:           .110 .... = Begin-End Data Message
NSP:           .... 00.. = Data Message
NSP:           .... ..00 = always zero
NSP:  Type      = 0  (Data Message)
NSP:  Sub-type = 6  (Begin-End Data Message)
NSP:  Logical Link Destination = 2830
NSP:  Logical Link Source      = 1410
NSP:  Acknowledge Number
NSP:     Acknowledge Qualifier     = ACK
NSP:     Message Number Acknowledged = 2

SP:  Segment Number = 2
NSP:   [76 data bytes]
NSP:
DAP:  ----- Data Access Protocol -----
DAP:
DAP:  Code = 2  (Attributes)  Operand Length = 29
DAP:  Attribute Data Type:   ASCII Data
DAP:  Attribute of File being Accessed = FB$SEQ;  Sequential
DAP:  Attribute Record Format          = FB$VFC;  Variable
with fixed control format
DAP:  Record Attribute Type:
DAP:     FB$PRN; Print file carriage control
DAP:  File Record Length  (bytes)      = 0
DAP:  Allocation Quantity in Blocks    = 26
DAP:  Size of Fixed Part of Variable Length = 2
DAP:  File Extension Quantum Size      = 0
DAP:  File Operation Attribute Type:
DAP:     FB$SQO; Sequential access only
DAP:  Node Access Attribute Type:
DAP:     FB$MDI; Directory structured
DAP:     FB$FOD; A file-oriented device
DAP:             Device can be shared
DAP:     FB$MNT; Device is currently mounted
DAP:     FB$IDV; Device is capable of providing input
DAP:     FB$ODV; Device is capable of providing output
DAP:     FB$AVL; Device is available for use
DAP:     FB$ELG; Device has error logging enabled
DAP:     FB$RAD; A random access device
DAP:  Longest Record Length            = 82
DAP:  Highest Virtual Block Allocated  = 26
DAP:  End of File Virtual Block Number = 26
DAP:  First Free Byte in End of File   = 150
DAP:
DAP:  Code = 15  (Name)  Operand Length = 39
DAP:  Name Type:   File Specification
DAP:  File Name Specification =
"SYS$SPECIFIC:[DECNET]NETSERVER.LOG;32"
DAP:
DAP:  Code = 6  (Acknowledge)
```

SUMMARY and DETAIL views of a packet, decoded by
The Sniffer's DECnet protocol interpreter.

Figure 2.

```
Frame   Delta t   From 7.45               From 7.52

 383    0.0556   DAP (File Attr) Open existing file SYS$SPECIFIC:[DECNET]NETSERVER....
 385    0.2712                            DAP (File Attr) Spec=SYS$SPECIFIC:[DEC....
 387    0.0142   DAP Connect
 389    0.0073                            DAP (Ack)
 391    0.0672   DAP Read
 394    0.7670                            DAP Data, 48 bytes <more...>
 395    0.0022                            DAP Data, [Middle, Len=1461]
 396    0.0017                            DAP Data, [End, Len=1154]
 400    0.1453                            DAP Data, 79 bytes <more...>
 401    0.0022                            DAP Data, [Middle, Len=1461]
 402    0.0018                            DAP Data, [End, Len=1207]
 412    5.4901                            DAP Data, 79 bytes <more...>
 439   10.5741                            DAP Data, 42 bytes <more...>
 441    0.0112                            DAP Data, [Middle, Len=1461]
 443    0.0120                            DAP Data, [End, Len=1225]
 445    0.0371                            DAP Data, 8 bytes Status=(5,47) <more...>
 456    5.3659                            DAP Data, 8 bytes Status=(5,47) <more...>
 472    5.1604   DAP End-of-stream
 474    0.0064                            DAP Response
 476    0.0112   DAP Close Terminate Access
 478    0.0213                            DAP Response
```

A high level, Data Access Protocol (DAP), SUMMARY view of a file transfer, revealing 5 and 10 second dead spots.

Figure 3.

```
Frame  Delta t  From 7.45       From 7.52

 383    0.0360  NSP DATA Begin-End D=1410  S=2830  ACK=1 SEG=2 LEN=60
 384    0.0018                NSP ACK  Data      D=2830  S=1410 ACK=2
 385    0.2694                NSP DATA Begin-End D=2830  S=1410 ACK=2 SEG=2 LEN=76
 386    0.0045  NSP ACK  Data      D=1410  S=2830  ACK=2
 387    0.0096  NSP DATA Begin-End D=1410  S=2830  ACK=2 SEG=3 LEN=5
 388    0.0019                NSP ACK  Data      D=2830  S=1410 ACK=3
 389    0.0054                NSP DATA Begin-End D=2830  S=1410 ACK=3 SEG=3 LEN=2
 390    0.0044  NSP ACK  Data      D=1410  S=2830  ACK=3
 391    0.0628  NSP DATA Begin-End D=1410  S=2830  ACK=3 SEG=4 LEN=6
 392    0.0020                NSP ACK  Data      D=2830  S=1410 ACK=4
 394    0.7650                NSP DATA Begin     D=2830  S=1410 ACK=4 SEG=4 LEN=1461
 395    0.0022                NSP DATA Middle    D=2830  S=1410 ACK=4 SEG=5 LEN=1461
 396    0.0017                NSP DATA End       D=2830  S=1410 ACK=4 SEG=6 LEN=1154
 398    0.0081  NSP ACK  Data      D=1410  S=2830  ACK=4
 399    0.0045  NSP ACK  Data      D=1410  S=2830  ACK=6
 400    0.1326                NSP DATA Begin     D=2830  S=1410 ACK=4 SEG=7 LEN=1461
 401    0.0022                NSP DATA Middle    D=2830  S=1410 ACK=4 SEG=8 LEN=1461
 402    0.0018                NSP DATA End       D=2830  S=1410 ACK=4 SEG=9 LEN=1207
 412    5.4901                NSP DATA Begin     D=2830  S=1410 ACK=4 SEG=7 LEN=1461
 413    0.0074  NSP ACK  Data      D=1410  S=2830  ACK=6
 414    0.0015  NSP DATA Link      D=1410  S=2830  ACK=1 SEG=2
 415    0.0019                NSP ACK  Oth-Data  D=2830  S=1410 ACK=2
```

The Network Services (NSP) layer of the DECnet protocol, SUMMARY view, where the problem is seen to reside in the lack of response from station 7.45.

NETWORK GENERAL CORPORATION
1945A Charleston Road
Mountain View, California 94043
Phone: (415) 965-1800
Fax: (415) 965-9608